IN THE UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF OHIO, EASTERN DIVISION

UNITED STATES OF AMERICA,	:	CASE NO. 1:16CR236
Plaintiff,	:	JUDGE PATRICIA A. GAUGHAN
v.	:	**MOTION TO DISMISS INDICTMENT**
	:	***Evidentiary Hearing Requested Oral Argument Requested***
ADAM LIBBEY-TIPTON,	:	
Defendant.	:	

Now comes the Defendant, Adam Libbey-Tipton, by and through undersigned counsel, Hector G. Martinez, Jr., Esq. and Leslie S. Johns, Esq., and respectfully moves this Honorable Court, pursuant to Fed.R.Crim.R. 12(A)(3) and the Court's supervisory powers, for an Order dismissing the indictment in this case, with prejudice, based on outrageous government conduct, for the reasons more fully set forth in the attached Memorandum in Support.

Respectfully submitted,

/s/ Hector G. Martinez, Jr.

/s/ Leslie S. Johns

HECTOR G. MARTINEZ, JR., Esq.
Sup. Ct. Reg. No. 0068832
LESLIE S. JOHNS, Esq.
Sup. Ct. Reg. No. 0092099
THE MARTINEZ FIRM
4230 State Route 306, Suite 240
Willoughby, OH 44094
Tel: (216)875-5555
Facsimile: (216) 875-5566
hector@martinezlawfirm.com
leslie@martinezlawfirm.com

Counsel for Defendant

INTRODUCTION

From February 19, 2015, through March 4, 2015, the United States Government was the world's largest distributor of child pornography on the Tor network. As part of "Operation Pacifier," the Government actively aided and abetted more than 100,000 users in posting, viewing, and sharing illegal pictures and videos. The FBI itself has distributed as many as 1,000,000 pictures and videos of child abuse, likely causing harms greater than that of any distribution defendant who has ever been prosecuted in this district.

This operation is impossible to reconcile with the Government's long-established position that each and every viewing of child pornography re-victimizes the abused child. Ironically, the prosecution of approximately 186 cases nationwide as a result of "Operation Pacifier" pales in comparison to the hundreds of thousands of re-victimizations that the FBI has enabled. Under Supreme Court precedent, the Court can and should dismiss the indictment in this case.

STATEMENT OF FACTS

On August 7, 2015, FBI agents assisted by local law enforcement executed a search warrant at the home of Adam Libbey-Tipton in Cleveland, Ohio. Mr. Libbey-Tipton is thirty (30) years old and is currently self-employed. The search was conducted pursuant to a warrant issued by the Honorable Gregory A. White. The warrant was based on an application prepared by FBI Special Agent Lisa Hack. Ex. A ("Residential Warrant").

As set forth in that application, the events leading to the search of Mr. Libbey-Tipton's home began on or about February 20, 2015, when the FBI took control of a website identified as "Website A" based in Virginia. Ex. A at ¶ 11. Website A is described as a "child pornography bulletin board and website decided to the advertisement and distribution of child pornography and the discussion of matters pertinent to the sexual abuse of children." *Id.* Based on the discovery and defense investigation to date, it appears that Website A offered a mix of discussion forums, private messaging services, both legal and illegal pictures and videos, and links to pictures and videos. *Id.* at ¶ 12. The discovery further indicates that site members resided throughout the United States and, most likely, many places abroad. Users accessed the site with a username and password, and they were instructed to avoid using personally identifying information when joining or communicating on the site. *Id.* at ¶¶ 12-13.

In addition, Website A operated on a network that is designed to protect user privacy and "facilitate anonymous communication over the Internet." *Id.* at ¶ 7. This network is commonly known as "the onion route" or "Thor" network, and is designed to route communications through multiple computers to protect the confidentiality of the internet protocol (IP) addresses and other identifying information of its users. *See id.* at ¶¶ 7-10; *see also* https://www.torproject.org ("Tor is free software and an open network that helps you defend against traffic analysis, a form of network surveillance that threatens personal freedom and privacy, confidential business activities and relationships, and state security.") The network was originally designed by the U.S. Naval Research Laboratory and is freely available to the public. The network is readily accessed by downloading free software and, like the Internet in general, it can be used for other legitimate and illicit purposes. *See* James Ball, *Guardian Launches Secure Drop System for Whistleblowers to Share Files*, The Guardian, June 5, 2014 (describing the newspaper's initiation of a secure means for whistleblowers to submit documents via the Tor network);[1] Virginia Heffernan, *Granting Anonymity*, N.Y. Times, December 17, 2010 ("Peaceniks and human rights groups use

[1] Available at: http://www.theguardian.com/technology/2014/jun/05/guardian-launchessecuredrop-whistleblowers-documents

Tor, as do journalists, private citizens, and the military, and the heterogeneity and farflungness of its users – together with its elegant source doe – keep it unbreachable.”)[2]

In this case, it appears from the discovery that a foreign law enforcement agency first identified Website A in December, 2014, and provided the FBI with an IP address associated with the website. This IP address had been captured during a period when there was a brief “misconfiguration of the server” that hosted the site, allowing investigators to collect site address information that would not normally have been publicly accessible. Following up on this information, the FBI identified and arrested the administrator of the site in February 2015. The FBI then took control of the site and continued to operate it for investigative purposes.

On February 20, 2015, the FBI submitted a search warrant application (“The NIT Application”) to Magistrate Judge Theresa Carroll Buchanan in the Eastern District of Virginia. *Exhibit A*. This application sought authorization to use Network Investigative Technique (“NIT”) to search any and all “activating computers,” which are the computers “of any user or administrator who logs into the TARGET WEBSITE by entering a username and password.” *Exhibit A* at Bates 0037 (“Attachment A”). The warrant application further stated that the NIT would seize information from the target computers that included their IP addresses; the type of operating systems on the computers; and whether the “NIT has already been delivered to the activating computer.” *Id*. at Bates 0038 (“Attachment B”). Elsewhere in the application, the NIT is broadly described as “computer instructions” that would be unknowingly downloaded by the unidentified target users when they access the site *Exhibit A* at ¶ 33.

The application further states that “in order to ensure technical feasibility and avoid detection of the technique by suspects under investigation” the NIT may be deployed against

[2] Available at: http://www.nytimes.com/2010/12/19/magazine/19FOB-Medium-t.html?_r=0

"any user who logs into the TARGET WEBSITE," regardless of the nature or extent of their activities in connection with the site. *Exhibit A* at Bates 0029, n. 8. While the application goes on to state that the FBI may elect to target particular users "more discretely," *id.*, it sought and obtained authorization to deliver the NIT to all of the tens of thousands of site members, regardless of their location or whether they are merely engaging in chat or bulletin board communications that did not involve the receipt or distribution of illegal images.

Further, the NIT application does not allege that anyone who visited the Target Website necessarily viewed or downloaded illegal pictures. In this regard, the application does not claim that the name of the site identifies it as a source of child pornography, and while the main page contained "two images depicting partially clothed pubescent girls with their legs spread apart," *Exhibit A* at ¶ 12, the application does not claim that these images are child pornography. The rest of the main page consists of instructions for registering an account and related information. *Id*. Moreover, once a user enters the site, he or she is presented with a variety of forums, including various chat rooms, "general discussion" and "security and technology" forums, and more explicitly labeled sections for such things as "Pre-Teen Videos" and "HC" (hardcore). *Exhibit A* at ¶¶ 14-17.

Finally, the FBI requested authorization to delay providing notification to the targets of the NIT search for a period of "30 days after any individual accessing the TARGET WEBSITE has been identified to a sufficient degree as to provide notice, unless the Court finds good cause for further delayed disclosure." *Exhibit A* at ¶ 40. The court granted this request for a period not to exceed 30 days and, from the available discovery, it appears that no extension of this delayed notice was requested or granted.

The FBI began "deploying" its NIT on February 20, the same day the IT warrant was granted. It appears form the discovery available to date that, in order to avoid revealing to potential targets that it had taken control of Website A, the FBI continued to distribute child pornography from the site. *See Exhibit B* (Residential Warrant) at ¶ 28 (stating that during the time the site was controlled by the Government a user later identified as Mr. Libbey-Tipton accessed a post on the site that contained a link to a video).

On or about March 3, 2015, the FBI surreptitiously sent the NIT to a computer connected to someone with the username "Revenger" and extracted its IP address and other identifying information. According to the July 31, 2015, application for a warrant to search Mr. Libbey-Tipton's home, "Revenger" had accessed a post that contained a link to a child pornography video. *Exhibit B* at ¶ 28. In addition, the residential application alleged that "Revenger" had previously been logged into the site for 34 hours, 13 minutes, and 24 seconds. *Id*. at 19. It appears from the discovery that none of this information was known to law enforcement before the NIT was deployed against "Revenger."

In March 2015, the FBI sent a subpoena to AT&T U-Verse for information related to the "Revenger" IP address that – through use of the NIT – had been seized on March 3, 2015. AT&T responded with Stacey Irace's subscriber information, including an address and preferred email address. *Id*. at ¶ 33.

On August 7, 2015, FBI made contact with Mr. Libbey-Tipton at his home. The agents advised Mr. Libbey-Tipton that they had the Residential Warrant issued by Judge White, but they did not disclose that his computer had previously been searched or provide him with a copy of the NIT warrant. Mr. Libbey-Tipton cooperated with the agents. Various computers, hard drives, and storage devices were seized pursuant to the Residential Warrant.

On July 27, 2016, an indictment was filed with this Court, charging Mr. Libbey-Tipton with possession of child pornography. On January 18, 2017, a superseding indictment was filed with this Court, charging Mr. Libbey-Tipton with Receipt or Distribution of Child Pornography. The indictments did not disclose the Title III warrant or the fact that Mr. Libbey-Tipton's computer had been searched by means of NIT. Defense counsel has served the Government with a comprehensive discovery request, including a request for copies of any search warrants and affidavits resulting in the seizure of evidence intended for use by the government at trial. The Government has disclosed the existence of the NIT warrant by providing a copy of it to the defense. Any Title III warrants have not been disclosed.

According to the discovery, approximately 100,000 users logged in to the site during the February 20 to March 4, 2015 time period. *See Exhibit C (United States v. Michaud,* CR15-05351RJB, dkt. 109 (Govt. Response to Order Compelling Discovery) at 4. There were approximately 1,000,000 total logins during the same time period (with some users logging in multiple times). *Id.*

Prior to the FBI's operation of the site, the average number of weekly visitors had been just 11,000. *See Exhibit B* ¶ 19. Despite several requests for an explanation, the Government refused to disclose how it increased the traffic to the FBI's site fivefold.

The FBI's operation of the site included facilitating the uploading and redistribution of child pornography onto the Internet. From a technical standpoint, these actions require the approval of, and substantial technical assistance from, whoever is administering a site that hosts pictures and videos.

The Government has not provided the exact distribution numbers involved in this enterprise. Instead, the Government has acknowledged that it distributed a minimum of 22,000 pictures, videos, and additional links to child pornography. *See Exhibit B* at 2-3. However, the Government has also maintained that it is unable to account for all of the content that was posted on its site. For example, according to the Government, most of the content was available only for a "limited time" and was not tracked by the FBI, and many of the links on the site contained multiple images and videos. *Id*. at 3.

Given the limited information that has been disclosed so far, a reasonable estimate that the FBI actually distributed somewhere in the range of 1,000,000 pictures and videos. As noted, there was a total of approximately 1,000,000 logins to the FBI's site (with some of the 100,000 users logging in multiple times). Assuming that the site was dedicated to child pornography as the Government has claimed, then it would be fair to assume that visitors downloaded or posted at least one picture or video during their visits. This results in a conservative estimate that the FBI distributed somewhere in the range of 1,000,000 images of child abuse.

The Government has also conceded that, unlike a typical "reserve sting" operation, law enforcement agents made no attempt to control or curtail the redistribution of any of the Playpen contraband. This is true despite the fact that the child pornography on the site was located in specific subdirectories and the FBI had the technical means of allowing visitors to access those parts of the site while blocking them from downloading any of the pictures found there.

LAW AND ARGUMENT

A. THE GOVERNMENT'S GLOBAL DISTRIBUTION OF CHILD PORNOGRPAHY IS OUTRAGEOUS CONDUCT THAT WARRANTS DISMISSAL OF THE INDICTMENT.

1. The Law Permits Dismissal of the Indictment in Cases Where the Government Acts in an Outrageous Fashion.

The remedy the defense is seeking is extraordinary, but only because the Government's conduct in this case is unprecedented and would appall the average citizen. Criminal investigations should seek to contain and mitigate the harm caused by illegal activity, not perpetuate that harm and (according to the Government's own often repeated statements) "re-victimize" the children depicted in the images that it distributed.

The Supreme Court has long held that the federal judiciary has the power to evaluate a criminal case's entire proceedings to determine whether they "offend those canons of decency and fairness which express the notions of justice of English-speaking peoples even toward those charged with the most heinous offenses." *Rochin v. California*, 342 U.S. 165, 169 (1952) (quoting *Malinski v. People of State of New York,* 324 U.S. 401, 416-17 (1945)). When the Government violates these standards of "decency and fairness" due process concerns are implicated. *See id*. Thus, government conduct that "shocks the conscience" may constitute a due process violation, requiring dismissal. *Rochin* at 172.

Government conduct that is so outrageous that it offends our shared canons of decency to a degree warranting dismissal of an indictment is rare, and the standard for dismissal on this ground is "extremely high." *United States v. Smith*, 924 F.2d 889, 897 (9th Cir. 1991). An indictment can be dismissed only where the Government's conduct is "so grossly shocking and so outrageous as to violate the universal sense of justice." *United States v. Stinson*, 647 F.3d 1196, 1209 (9th Cir. 2011) (quoting *United States v. Restrepo,* 930 F.2d 705, 712 (9th Cir. 1991))*; accord, United States v. Pedrin,* 797 F.3d 792, 795–96 (9th Cir. 2015) (quoting *Stinson).* The facts surrounding *"Operation Pacifier"* meet that standard.

2. The Government has Long Argued that Possession or Distribution of Child Pornography is a Heinous Crime.

The Court should find that the Government's conduct during the investigation of this case warrants dismissal. While other potential remedies have been presented to the Court through Defendant's Motions to Suppress, an order merely excluding evidence would not adequately convey the level of disapproval with which the FBI's actions should be met. The Court need only consider some of the Government's own pronouncements about the harm caused by the proliferation of child pornography to fully realize how troubling "Operation Pacifier" is as it was implemented. While the defense does not necessarily agree with some of the Government's more extreme statements about the impact of downloading or distributing illicit pictures, it is impossible to reconcile the Playpen operation with the Government's own view of the harm caused by the distribution of child pornography.

For example, the Department of Justice's website states the following:

> [V]ictims of child pornography suffer not just from the sexual abuse inflicted upon them to produce child pornography, but also from knowing that their images can be traded and viewed by others worldwide. *Once an image is on the Internet, it is irretrievable and can continue to circulate forever.* The permanent record of a child's sexual abuse can alter his or her live (*sic*) forever. Many victims of child pornography suffer from feelings of helplessness, fear, humiliation, and lack of control given that their images are available for others to view in perpetuity.[3]

(Emphasis added). DOJ also routinely emphasizes in its press releases that possessing and circulating pornographic images re-victimizes the children depicted in them. *See, e.g.*, DOJ Press Release, *Ellettsville Man Charged with Production of Child Pornography*, April 15, 2015 ("Producing and distributing child pornography re- victimizes our children every time it is passed from one person to another").[4]

---

[3] Available at: http://www.justice.gov/criminal-ceos/child-pornography. This statement appears as part of the mission statement for the Child Exploitation and Obscenity Section (CEOS), which apparently approved and supervised the Playpen operation.

[4] Available at: http://www.justice.gov/usao-sdin/pr/ellettsville-man-charged-production-child-pornography.

Indeed, the Government has expressed the view that even looking at an image of child pornography re-victimizes children. *See, e.g.,* FBI.gov, *Defendant Sentenced for Possession of Child Pornography*, November 5, 2013 (justifying a 108 month sentence or a U.S. Air Force airman who possessed child pornography on the ground that "he caused the young children in these disgusting images to be re-victimized every time he looked at the pictures.").[5] More recently, *see* Dept. of Justice, Federal and State Authorities Charge 11 Men with Trading Child Pornography (Apr. 6, 2016) (quoting FBI supervisor stating "[t]he children depicted in these images that were illegally shared are victimized time and time again.").[6]

The harm caused by simply possessing, let alone distributing, illegal pictures is one that is also routinely emphasized by the Government. In fact, the Supreme Court has fully embraced that logic, explaining that circulating child pornography "renew[s] the victim's trauma" and makes it difficult for victims to recover from abuse. *Paroline v. United States*, 134 S. Ct. 1710, 1717 (2014) (victim's suffering was "compounded by the distribution of images of her abuser's horrific acts, which meant the wrongs inflicted upon her were in effect repeated; for she knew her humiliation and hurt were and would be renewed into the future as an ever-increasing number of wrongdoers witnessed the crimes committed against her"); *see also, e.g., United States v. Gilliam*, CR13-5028RJB, Dkt. 48 (Govt. Sentencing Memo) at 6 ("Every participant in the chain – producer, distributor, consumer – sustains the market for these images, and each victim, whether identified or not, suffers not only when an image is created, but each and every time an image is viewed").

---

[5] https://www.fbi.gov/atlanta/press-releases/2013/defendant-sentenced-for- possession-of-child-pornography. It should be noted here that several studies have determined that most child pornography possession and distribution offenders have no history of molesting minors and pose no significant future risk of doing so in the future. *See, e.g.*, Endrass et al, *The Consumption of Internet Child Pornography and Violent Sex Offending*, BMC Psychiatry (2009).

[6] Available at https://www.justice.gov/usao-cdca/pr/federal-and-state-authorities- charge-11-mentrading-child-pornography-through-use-peer.

Indeed, in recent pleadings, the Government has insisted that the people who run child pornography sites are more culpable than people who view the pornography. According to the Government itself, site operators make the pornography available to far more people than average picture collectors and they "directly participate" in an illegal marketplace.[7]

The Government has also emphasized that maintaining a child pornography website "encourages" the production and circulation of new pornography. In this case, the FBI has apparently made no effort to determine if the pictures and videos posted on Playpen while under its control were "known" images that had been previously circulated or if it was aiding and encouraging the production and distribution of new images. The FBI's conduct is all the more troubling in light of the fact that it somehow managed to increase the number of visitors to Playpen while it was under Government control from an average of 11,000 weekly visitors to approximately 50,000 per week.

3. The Ends of this Investigation Cannot Justify the Means.

The issue here is how, while decrying the long-term and widespread consequences to victims of allowing someone to even view illicit images, the Government can justify its massive distribution of child pornography. It is no answer that the FBI did this as part of an effort to apprehend people. That end does not (and was never going to) justify the means. This is simply because the FBI could not investigate, much less prosecute, 100,000 or so Playpen visitors in a timely fashion. Predictably, the Government ended up spreading far more child pornography, and enabled many more crimes, than it could ever investigate and prosecute.

---

[7] A copy of the sealed sentencing memo in which these points appear can be made available to the Court upon request.

Moreover, as a practical matter, the FBI had other ways of targeting Playpen visitors who wanted to access illegal content. For example, in other investigations, the FBI has monitored child pornography sites and posted links to pictures or videos with explicit titles. When a visitor to the forum clicked on a link, a "Network Investigative Technique" could seize identifying data about the visitor, but the link itself would be blocked or an "error" message would appear.

Alternatively, investigators can use a "spoofing" system, where visitors to a target site are secretly redirected to a server with a facsimile of the site, minus any content or links that investigators do not want accessible or downloadable. The Government has also used child erotica or "virtual" child pornography to lure targets in other cases, which would address any concerns agents might have had about "tipping off" suspects if sexual content was removed from the site entirely. *See* Corey Young, *FBI Allowed for More Victimization by Permitting a Child Pornography Website,* The New York Times (January 27, 2016) (discussing some of the investigatory alternatives and criticizing the "immoral and inexcusable" Playpen operation).[8]

Worse yet, the Government maintains that it was authorized to search the personal computers of anyone who merely visited Playpen's home page. If that is true, there was no investigatory need for the FBI to allow visitors to post new child pornography on the site or download the pornography that was available in specific subdirectories.

While law enforcement agents often use contraband, like drugs or guns, as part of undercover "buys" or to execute a sting operation, they only do so when necessary. They also make every effort to control, track and recover the contraband they are using. Here, by contrast, what the Government did is comparable to flooding a neighborhood with heroin in the hope of snaring an assortment of low-level drug users.

---

[8] Available at: http://www.nytimes.com/roomfordebate/2016/01/27/the-ethics-of-a-child-pornography-sting/fbi-allowed-for-more-victimization-by-permitting-a-child- pornography-website.

Given these facts, Operation Pacifier bears a striking resemblance to the "Fast and Furious" scandal. There, federal agents allowed guns to pass into the hands of gun smugglers and perpetuated the very crimes they were supposed to be preventing. *See* Dept. of Justice, Office of the Inspector General, *A Review of the ATF's Operation Fast and Furious and Related Matters* (Sept. 2012) (criticizing DOJ's handling of "gun walk" investigations that resulted in the uncontrolled distribution of firearms). As one senior agent told Congress at the time, "What the persons approving this debacle failed to realize is that the end does not justify the means." *See* Katherine Eban, *The Truth About the Fast and Furious Scandal*, Fortune, June 27, 2012 (detailing how these type of investigations require senior approval and some of the disciplinary consequences that flowed from the debacle).

That lesson appears to have been lost on the FBI, even as it seeks to vastly expand its power to investigate cybercrimes. Absent at least additional discovery and a full evidentiary hearing on this motion, the Government may well any avoid public accountability for its actions.

4. Federal Law Explicitly Forbids the Government from Distributing Child Pornography.

The Government's conduct was not just morally reprehensible, it was flatly illegal. There is no statute that allows the Government to distribute child pornography, regardless of the circumstances. In addition, multiple statutes govern how law enforcement is permitted to interact with such materials. None allow for its distribution, even as part of a misguided "reverse sting."

For instance, 18 U.S.C. § 3509(m) expressly requires that "any property that constitutes child pornography . . . shall remain in the care, custody and control of the Government" or a court. As a rule, defense counsel cannot independently possess such images, even subject to a protective order. Attorneys have even been charged and sued civilly for making fake child pornography as trial exhibits. *See* Pat Murphy, *Court: Lawyer must play $300k for child porn trial exhibits*, Detroit Legal News (Nov. 22, 2012).[9]

Other statutes addressing the Government's duties with regard to child pornography include 18 U.S.C. § 1466A(e), 18 U.S.C. § 2252(c), 18 U.S.C. § 2252A(c) and 18 U.S.C. § 2258C(d)-(e). None of these provisions permit the Government to publicly distribute that material. And given that Playpen was open to anyone all over the world, the Government likely violated dozens of international child pornography laws as well. *See, e.g.,* R.S.C. 163.1(3) (Canadian law barring distribution of child pornography); Protection of Children Act, 1978, 1(1)(b) (same, United Kingdom).

5. The Government Also Violated its own "Investigative Principles."

Online investigations are especially sensitive and problematic because agents have no ability to control the redistribution of pictures, malware or other contraband once they are introduced to the Internet. As a result, the Department of Justice (DOJ) itself cautions its attorneys and agents about the harms that can arise from online investigations and requires special approval for operating any type of "online undercover facility." DOJ, *Online Investigative Principles for Federal Law Enforcement Agents* (available at: https://info.publicintelligence.net/DoJ-OnlineInvestigations.pdf). DOJ's investigative principles emphasize that law enforcement agencies must consider several sensitive issues when determining whether to approve the establishment of an online undercover facility:

> First, online undercover facilities that offer the public access to information or computer programs that may be used for illegal or harmful purposes may have greater capacity than similar physical-world undercover entities to cause unintended harm to unknown

[9] Available at http://www.legalnews.com/detroit/1369660.

> third parties. ***Because digital information can be easily copied and communicated, it is difficult to control distribution in an online operation and so limit the harm that may arise from the operation***.

Id. at 44 (p. 57 of the PDF) (emphasis added).

The statement of principles goes on to caution that the use of online undercover facilities raises complex legal and policy issues, "especially if law enforcement agents seek to use the system administrator's powers for criminal investigative purposes." These include "unique and sensitive policy issues involving privacy, international sovereignty, and unintended harm to unknown third parties." *Id*. at x (p. 11 of the PDF).

Because of these concerns, DOJ requires any investigation involving an online undercover facility to undergo a special review and approval process. *Id*. The Government has refused to disclose its review and approval records in this case. DOJ's guidelines also compares online "sting" operations with other operations employing tools of criminality. Using an example of selling "cloned phones," DOJ pointed out that agents "can prevent or minimize the potential for harm caused by their activities by, for example, arresting targets before they can use the phones or requesting the cellular carrier to block or limit access by these particular phones to the cellular network." *Id*. at 44 (p. 57 of the PDF). Even when that cannot occur, the harm is constrained by the fact that "a single 'clone phone' can only be used by one individual at a time and cannot be duplicated and redistributed to multiple users." *Id.* Similar limits, however, are difficult or impossible to impose on online undercover operations, as DOJ cautions in its policy statement:

> [T]he online facility is likely to be automated, making it difficult for the agents to limit who obtains the tools or the damage that the tools end up causing to innocent third parties. Further, unlike the clone phone, the hacker tools can be ***endlessly replicated and***

> ***distributed to others in a manner that law enforcement agents cannot easily control.***

Id. at 45 (p. 58 of PDF) (emphasis added).

In this case, the FBI took no measures whatsoever to control the replication and distribution of pictures and videos from its undercover website. It also appears from the available discovery that the FBI did not identify or make timely reports to the National Center for Missing and Exploited Children about any new images of child abuse that were introduced through Playpen.

6. The Government Has Refused to Meet its Statutory Restitution Obligations to Victims.

Finally, the Government has so far denied that it has any responsibility to the victims depicted in the pictures that it has distributed. Its own mission statements explain that it harmed the lives and mental health of thousands of victims by distributing child pornography. Accordingly, like any entity that distributes or possesses child pornography, it has an absolute statutory obligation under 18 U.S.C. § 2255 to make restitution to known victims. An evidentiary hearing on this motion will help provide victims with the facts and notice that will allow them to seek restitution.

CONCLUSION

For the reasons stated above, the Court should schedule an evidentiary hearing to determine the extent of the harm caused by the Government's investigatory tactics and dismiss the indictment if the Court finds that the governmental conduct leading to the charges against the defendants cannot be reconciled with fundamental expectations of decency and fairness.

Dated this 20th day of March, 2017.

Respectfully submitted,

/s/ Hector G. Martinez, Jr.

/s/ Leslie S. Johns
HECTOR G. MARTINEZ, JR., Esq.
LESLIE S. JOHNS, Esq.
Counsel for Defendant

CERTIFICATE OF SERVICE

I hereby certify that a copy of the foregoing was served this 20th day of March 2017 by regular U.S. mail postage prepaid and electronic mail upon:

Brian M. McDonough, Esq.
Assistant United States Attorney
United States Court House
801 West Superior Avenue, Suite 400
Cleveland, Ohio 44113

/s/ Hector G. Martinez, Jr.

/s/ Leslie S. Johns
HECTOR G. MARTINEZ, JR., Esq.
LESLIE S. JOHNS, Esq.
Counsel for Defendant